ATTACHMENT A

Statement Of Facts

The following Statement of Facts is incorporated by reference as part of the Plea Agreement between the Department of Justice, Criminal Division, Money Laundering and Asset Recovery Section ("MLARS"), and the United States Attorney's Office for the District of New Jersey (the "USAO-DNJ") (collectively, the "Offices"), and TD BANK US HOLDING COMPANY ("TDBUSH") and TD BANK, NATIONAL ASSOCIATION ("TDBNA" or the "Bank") (collectively, the "Defendants"). The Defendants hereby agree and stipulate that the following facts are true and accurate. Certain of the facts herein are based on information obtained from third parties by the United States through its investigation and described to the Defendants.

The Defendants admit, accept, and acknowledge that they are responsible for the acts of their officers, directors, employees, and agents as set forth below. Had this matter proceeded to trial, the Defendants acknowledge that the United States would have proven beyond a reasonable doubt by admissible evidence the facts alleged below and set forth in the Criminal Informations.

Overview

1. TDBNA, which markets itself as "America's Most Convenient Bank," is the tenth largest bank in the United States. Headquartered in Cherry Hill, New Jersey, the Bank has over 1,100 branches, or what TDBNA calls "stores," along the eastern seaboard of the United States, including a large presence in New Jersey, New York, and Florida. Throughout the relevant period, as defined below, TDBNA's retail banking activity involved providing banking products and services (e.g., checking and savings accounts, debit cards, and loans) to over 10 million individual and commercial customers in the United States.

2. TDBUSH, the direct parent of TDBNA, has oversight of the Bank's anti-money laundering ("AML") compliance program, including through reporting to TDBUSH's Audit Committee, and is accountable for monitoring the effectiveness of the Bank's AML program pursuant to the Bank Secrecy Act ("BSA"). TDBUSH in turn is the wholly owned subsidiary of TD Group US Holdings LLC ("TDGUS"), which is the intermediate holding company and ultimate parent holding company in the United States. TDGUS is responsible for oversight of the risk management framework for all U.S. operations, including AML programs. TDGUS is a wholly owned subsidiary of the Toronto-Dominion Bank d/b/a TD Bank Group, an international banking and financial services corporation located in Canada. TD Bank Group is the ultimate parent bank of all TD operations. Together, TDBNA, TDBUSH, TDGUS, and TD Bank Group, and their affiliates and subsidiaries, are referred to herein as TD or the Group.

3. Between January 2014 and October 2023 (the "relevant period"), TDBNA and TDBUSH failed to maintain an AML program that complied with the BSA and prioritized a "flat cost paradigm" across operations and the "customer experience." As a result, the Defendants willfully failed to remediate persistent, pervasive, and known deficiencies in its AML program, including (a) failing to substantively update its transaction monitoring system, which is used to detect illicit and suspicious transactions through the Bank, between 2014 and 2022 despite rapid growth in the volume and risks of the Bank's business and repeated warnings about the outdated system, and (b) failing to adequately train its employees who served as the first line of defense against money laundering. These failures enabled, among other things, three money laundering networks to launder over $600 million in criminal proceeds through the Bank between 2019 and 2023. These failures also created vulnerabilities that allowed five Bank store employees to open and maintain accounts for one of the money laundering networks. These five Bank employees

ultimately conspired with criminal organizations to open and maintain accounts at the Bank that were used to launder $39 million to Colombia.

4. TDBUSH's conduct, as described herein, constituted: (i) the willful failure to maintain an adequate AML program, in violation of Title 31, United States Code, Sections 5318(h) and 5322; and (ii) the knowing failure to accurately report currency transactions as required by the Secretary of the Treasury, in violation of Title 31, United States Code, Sections 5313 and 5324.

5. TDBNA's conduct, as described herein, constituted a conspiracy to: (1) willfully fail to maintain an appropriate AML program, contrary to Title 31, United States Code, Sections 5318(h), 5322; (2) knowingly fail to file accurate Currency Transaction Reports ("CTRs"), contrary to Title 31, United States Code, Sections 5313 and 5324; and (3) launder monetary instruments, contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i), all in violation of Title 18, United States Code, Section 371.

6. During the relevant period, Defendants willfully failed to maintain an adequate AML program at the Bank. At various times, high-level executives including those in Global AML Operations, in senior executive management, and on the TDBUSH Audit Committee—specifically including an individual who became Defendants' Chief Anti-Money Laundering Officer ("Chief AML Officer") during the relevant period (Individual-1) and the Bank's BSA Officer (Individual-2)—knew there were long-term, pervasive, and systemic deficiencies in the Defendants' U.S. AML policies, procedures, and controls. The Defendants did not substantively update the Bank's automated transaction monitoring system from at least 2014 through 2022—including to address known gaps and vulnerabilities in the TDBNA's transaction monitoring program—despite increases in the volume and risk of its business and significant changes in the nature and risk of transactional activity. In addition, during the relevant period, TDBNA monitored only

approximately 8% of the volume of transactions because it omitted all domestic automated clearinghouse ("ACH") transactions, most check activity, and numerous other transaction types from its automated transaction monitoring system. Due to this failure, the Bank did not monitor approximately $18.3 trillion in activity between January 1, 2018, through April 12, 2024. At the same time, Bank senior executives repeatedly prioritized the "customer experience" over AML compliance and enforced a budget mandate, referred to internally as a "flat cost paradigm," that set expectations that all budgets, including the AML budget, would not increase year-over-year. The Defendants' failures to appropriately fund the Bank's AML program and to adapt its transaction monitoring program resulted in a willfully deficient AML program that allowed three money laundering networks to exploit the Bank and collectively transfer over $670 million through TDBNA accounts. At least one scheme had the assistance of five store insiders at TDBNA.

7. From at least in or around January 2019 through in or around March 2021, the Defendants willfully failed to file accurate CTRs related to one of these three money laundering schemes. Da Ying Sze, a/k/a David ("David"), used TDBNA in furtherance of a money laundering and unlicensed money transmitting scheme for which he ultimately pled guilty in 2022. David conspired to launder and transmit over $653 million, of which more than $470 million was laundered through the Bank. David bribed Bank employees with more than $57,000 in gift cards in furtherance of the scheme. David laundered money through the Bank by depositing large amounts of cash—occasionally in excess of one million dollars in a single day—into accounts opened by other individuals and by requesting that Bank employees send wires and issue official checks. TDBNA failed to identify David as the conductor of transactions in over 500 of the CTRs the Bank filed for his transactions, totaling over $400 million in transaction value, despite David

entering TDBNA stores with nominee account holders and conducting transactions directly by making large cash deposits into accounts he purportedly did not control.

8. During the relevant period, TDBNA employed five individuals who provided material assistance, often in return for a fee, to a second money laundering scheme, which involved laundering tens of millions of dollars from the United States to Colombia. Insider-1 was a former Financial Service Representative at a TDBNA store in New Jersey. Insider-2 was a former Retail Banker at a TDBNA store in southern Florida. Insider-3 was a former Retail Banker at another TDBNA store in southern Florida. Insider-4 was a former Assistant Store Manager at a TDBNA store in eastern Florida. Insider-5 (jointly, the "TDBNA Insiders") was a former Store Supervisor at another TDBNA store in southern Florida. These insiders opened accounts and provided dozens of ATM cards to the money laundering networks, which these networks used to launder funds from the United States to Colombia through high volume ATM withdrawals. The insiders assisted with maintaining accounts by issuing new ATM cards and resolving internal controls and roadblocks, including freezes on certain account activity. Through the accounts the insiders opened, the money laundering networks laundered approximately $39 million through the Bank. Despite significant internal red flags, the Defendants did not identify the role the insiders played in the money laundering activity until law enforcement arrested Insider-1 in October 2023.

9. From March 2021 through March 2023, another money laundering organization that purported to be involved in the wholesale diamond, gold, and jewelry business ("MLO-1") maintained accounts for at least five shell companies at TDBNA and used those accounts to move approximately $123 million in illicit funds through the Bank. Since their account openings in 2021, TDBNA knew that these shell companies were connected because they shared the same account signatories. Despite these red flags, TDBNA did not file a Suspicious Activity Report ("SAR") on

MLO-1 until law enforcement alerted TDBNA to MLO-1's conduct in April 2022. By that time, MLO-1's accounts had been open for over 13 months and had been used to transfer nearly $120 million through TDBNA.

The Bank Secrecy Act and Other Relevant Legal Background

10. TDBNA is a national bank in the United States that is insured under the Federal Deposit Insurance Act and regulated and supervised by the Office of the Comptroller of the Currency ("OCC"). The Bank is therefore a financial institution for purposes of Title 31, United States Code, Section 5318(h).

11. The BSA, Title 31, United States Code, Section 5311, et seq., requires financial institutions—including TDBNA—to establish, implement, and maintain risk-based anti-money laundering programs to combat money laundering and the financing of terrorism through financial institutions.

12. The BSA requires that these AML programs, at a minimum, address five core pillars: (a) internal policies, procedures, and controls designed to guard against money laundering; (b) an individual or individuals responsible for overseeing day-to-day compliance with BSA and AML requirements; (c) an ongoing employee training program; (d) an independent audit function to test compliance programs; and (e) a risk-based approach for conducting ongoing customer due diligence. 31 U.S.C. § 5318(h); *see also* 31 C.F.R. § 1020.210.

13. To satisfy the BSA's requirements, a bank's AML program must be risk-based and its systems for identifying suspicious activity must be tailored to effectively monitor its customer-base and the products and services it offers, and reporting suspicious activity as required under the BSA. Moreover, a bank's AML policies, procedures, and controls must be calibrated to address

emerging and evolving risk, including risk associated with new products and services and new patterns of criminal activity.

14. For financial institutions of TDBNA's size and sophistication, an effective automated transaction monitoring system is necessary to properly identify, mitigate, and report suspicious activity as required by law and to prevent the institution from being used to facilitate criminal activity. Automated transaction monitoring systems filter transactions through a series of scenarios, or rules, in order to isolate a transaction or series of transactions with heightened indicia of money laundering, terrorist financing, or other illicit activity. If a transaction or series of transactions meet the parameters of a specific scenario, the automated transaction monitoring system generates an alert. Analysts then review each alert to determine whether the transaction was in fact suspicious and, if so, whether it should be escalated for further investigation or for the filing of a SAR with the United States Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), as required by the BSA. *See* 31 U.S.C. § 5318(g); 31 C.F.R. § 1020.320.

15. Under the BSA and its implementing regulations, financial institutions are also required to submit CTRs to FinCEN for "each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than $10,000." 31 C.F.R. § 1010.311. Banks must file the CTR with FinCEN "within 15 days following the day on which the reportable transaction occurred," and must include "[a]ll information called for" in the "forms prescribed." 31 C.F.R. §§ 1010.306(a)(1), (a)(3), (d). The BSA describes CTRs as the types of "reports or records that are highly useful in . . . criminal . . . investigations," 31 U.S.C. § 5311, as they help establish a paper trail for law enforcement to identify large currency transactions, recreate financial transactions, and identify conductors and beneficiaries.

16. As part of the obligation to report currency transactions above $10,000, a financial institution must "verify and record the name and address of the individual presenting a transaction, as well as record the identity, account number, and the social security or taxpayer identification number, if any, of any person or entity on whose behalf such transaction is to be effected." 31 C.F.R. § 1010.312. Therefore, a bank is required to identify in its CTR filing the person who conducted the transaction (i.e., the conductor) in addition to the account holder. *See* 31 U.S.C. § 5313(a); FinCEN Form 104 (March 2011).

TDBNA and TDBUSH's Failure to Maintain an Adequate AML Program

Background Regarding TDBNA's BSA/AML Program

17. TD Bank Group is a publicly traded (NYSE: TD) international banking and financial services corporation headquartered in Toronto, Canada. TD Bank Group is one of the thirty largest banks in the world and the second-largest bank in Canada. TD Bank Group's board is responsible for the supervision of the Group overall including major strategies, enterprise risk, executive hiring, and oversight of all subsidiaries. TD Bank Group's board oversees and monitors the integrity and effectiveness of the Group's internal controls and adherence to applicable compliance standards and is responsible for "setting the tone at the top as it relates to integrity and culture . . . and communicating and reinforcing the compliance culture throughout the [Group]."

18. TDGUS, incorporated in Delaware, is a wholly owned subsidiary of TD Bank Group. TDBUSH, which owns TDBNA, is a wholly owned subsidiary of TDGUS. Throughout the relevant period, TDBUSH and its Audit Committee oversaw TDBNA's BSA/AML program, including issuing the BSA/AML Policy and Standards, approving the appointment of the BSA Officer, and receiving reporting and briefing on all AML program matters. According to TDBUSH's BSA/AML Policy, "[t]he TDBUSH Board has ultimate responsibility for oversight of the [BSA/AML] Program and is accountable for monitoring its effectiveness regularly."

TDBUSH's responsibilities included "[s]etting the 'tone from the top' commitment; and [p]articipating in briefings regarding inherent risks and controls, so that Board members attain an adequate level of understanding, as well as challenging the information presented to them about the [BSA/AML] Program matters."

19. During the relevant timeframe, TD Bank Group operated an AML program that applied across the global bank through the Global Anti-Money Laundering ("GAML") group. GAML established TD Bank Group's AML policies and procedures, decided issues related to AML budgeting and staffing Group-wide, and oversaw "shared services" groups that served both the U.S. and Canadian AML programs, including the AML technology team and AML Operations. GAML was led by the Chief AML Officer, to whom the BSA Officer and other senior AML executives reported. AML Operations, a group that served both U.S. and Canadian operations, encompassed both the U.S. and Canadian Financial Intelligence Units ("FIUs") at the Bank, which, among other critical functions, carried out the identification and reporting of suspicious activity. The head of the U.S. FIU had dual reporting lines to the BSA Officer and the Vice President, AML Operations, who, in turn, each reported directly to the Chief AML Officer. Therefore, some of TD Bank Group's AML functions were centralized and others were separated between the U.S. and Canada. (The U.S. AML program is referred to herein as "US-AML.")

20. During the relevant period, TDBNA had elements of an AML program that appeared adequate on paper. TDBNA had a BSA Officer who had relevant AML credentials; maintained policies and procedures targeting money laundering, terrorist financing, violations of U.S. sanctions, and other illicit activity; and implemented some controls necessary for the identification and reporting of suspicious activity. Despite these efforts, however, there were

fundamental, pervasive flaws in the Bank's transaction monitoring program, which created an environment that allowed financial crime to flourish.

21. Individual-1, whose identity is known to the Offices and Defendants, was the Group's senior AML executive during all of the relevant period. TDBNA hired Individual-1 in 2013 as the VP, AML Operations, reporting directly to the then Chief AML Officer. In approximately 2017, Individual-1 was promoted to Co-Head of Global AML and thereafter effectively shared the Chief AML Officer responsibilities with another individual. In early 2019, Individual-1 became the sole Chief AML Officer, a position he held until 2023. As both the Co-Head of GAML and the Chief AML Officer, Individual-1 was responsible for TD's Group-wide AML program, which included establishing the annual Group-wide AML budget, setting GAML priorities, spearheading GAML's strategic planning, and regularly briefing the TD Bank Group and TDBNA boards of directors on AML compliance matters. Individual-1, as Chief AML Officer, also had specific oversight responsibilities related to US-AML, including oversight of TDBNA's BSA Officer; oversight of AML technology services, which was shared between the U.S. and Canada; and shared oversight, with the BSA Officer, of the U.S. FIU.

22. Individual-2, whose identity is known to the Offices and the Defendants, was an AML executive at TDBNA for nearly the entire relevant period. Individual-2 joined TDBNA in 2014 as Head of the U.S. FIU and, in that role, supervised the investigative teams responsible for reporting suspicious activity, filing CTRs, managing high-risk customers, and preventing sanctioned transactions. In January 2018, Individual-2 was promoted to Deputy BSA Officer and, in May 2019, assumed the roles of BSA Officer and Deputy Global Head of AML Compliance, which Individual-2 held until May 16, 2023. As BSA Officer, Individual-2 was responsible for US-AML, including establishing the budget and managing staffing, assessing the Bank's AML

risk, approving policies and procedures, and presenting to the TDGUS and TDBUSH boards of directors. In practice, Individual-2 was required to obtain approval from the Chief AML Officer, Individual-1, for the US-AML annual budget, as well as for all hiring decisions. Because the AML technology group reported directly to the Chief AML Officer, Individual-2 believed that issues related to US-AML technology were outside of Individual-2's supervision.

23. From 2016 through 2022, Individual-3, whose identity is known to the Offices and the Defendants, was a vice president and senior manager within AML Operations for TDBNA. Individual-3 also informally served as Head of the U.S. FIU from in or around 2017, when Individual-2 left that role, until a replacement was hired in or around December 2018. In AML Operations, Individual-3 oversaw various components of the U.S. FIU's AML functions, including the teams tasked with the initial review of transaction monitoring alerts and with managing Unusual Transaction Referrals ("UTRs"), which were reports of potentially suspicious conduct submitted by employees through TDBNA's internal reporting system.

Transaction Monitoring Issues Were Repeatedly Identified to TDBNA

24. Over at least the past eleven years, the OCC, FinCEN, TDBNA Internal Audit, and third-party consultants have repeatedly identified TDBNA's transaction monitoring program as an area of concern. The senior executive leadership and boards of directors of TDBNA, TDBUSH, TDGUS, and TD Bank Group were made aware of certain of the concerns identified by these regulators and auditors.

25. On September 23, 2013, the OCC and FinCEN announced enforcement actions against TDBNA carrying a combined civil monetary penalty of $37.5 million for violations of the BSA stemming from a Ponzi scheme orchestrated by a Florida attorney. TDBNA's board and the then-head of TDBNA signed the 2013 OCC Agreement. Despite the numerous AML alerts generated by its transaction monitoring program, TDBNA failed to timely identify and report

approximately $900 million in suspicious activity related to the scheme. According to FinCEN, TDBNA's failures were due, in part, to inadequate AML training for both AML and retail personnel. In announcing the resolution, the FinCEN Director noted, "[i]t is not acceptable to have a poorly resourced and trained staff overseeing such a critical function."

26. TDBNA failed to effectively or substantively adapt its transaction monitoring system after the 2013 enforcement actions. For example, in 2013, the OCC determined that TDBNA needed to develop transaction monitoring policies and procedures to ensure systematic and prompt responses to environmental or market-based changes, i.e., policies and procedures concerning the development of new transaction monitoring scenarios or manual processes to appropriately mitigate emerging risks. In 2018, the OCC characterized TDBNA's planning, delivery, and execution of AML technology systems and solutions as insufficient. Specifically, the OCC highlighted the delays in implementing multiple AML technology projects and found those delays to be directly linked to nearly all of TDBNA's outstanding AML program issues.

27. In 2018, TDBNA Internal Audit, which periodically assessed the Bank's AML program and specific functions within US-AML, determined that TDBNA's high-risk jurisdiction transaction monitoring scenarios were using an outdated list of high-risk jurisdictions, meaning the bank's scenarios were not designed to generate alerts on the jurisdictions currently deemed to be high risk. In 2020, TDBNA Internal Audit identified AML compliance deficiencies related to the governance and review of transaction monitoring scenarios, including that: (i) TDBNA lacked formal timelines for completing its scenario reviews, many of which had remained outstanding since 2017; (ii) TDBNA had not implemented its proposed changes to U.S. scenarios from the previous year; and (iii) TDBNA had no "procedure or formal document outlining the process to follow nor factors/trigger points for the promotion of new scenarios in [the transaction monitoring

system] or in a manual environment." The third finding, regarding the lack of governance of transaction monitoring scenario development, involved the same issues as the OCC finding from seven years earlier. All of these findings remained unresolved during the following year's TDBNA Internal Audit review. The Defendants' boards were informed of Internal Audit findings and associated remediation plans.

28. During the relevant period, TDBNA also engaged third-party consultants who identified fundamental weaknesses in the Bank's AML program, which were reported to GAML leadership. For example, in 2018, one consultant commented that "increased volumes and regulatory requirements" would put pressure on AML operations to meet demands and deadlines. The same consultant concluded that the Bank's required testing of its transaction monitoring scenarios—which assessed whether scenarios were adequately capturing suspicious activity—took twice as long as the industry average. In 2019, another consultant found that TDBNA had "sub-optimal [transaction monitoring] scenarios" due, in part, to "outdated parameters" that generated a large volume of alerts that limited "GAML's ability to focus on high risk customers and transactions." In 2021, a third consultant identified numerous limitations in the Bank's transaction monitoring program, including technology barriers to developing new scenarios or adding new parameters to existing scenarios.

TDBNA Failed to Update its Transaction Monitoring Program, Despite Known Gaps, Leaving Trillions of Dollars of Customer Activity Entirely Unmonitored

29. An effective AML transaction monitoring program must be capable of adapting to changes in the banking industry, including new methods of money laundering and new banking products and services. Indeed, in September 2021, Individual-2 informed the boards of directors for TD Bank Group, TDGUS, and TDBUSH that, "included within GAML's responsibilities is to

have an appropriate framework in place to identify and monitor both emerging and evolving risk." Yet over the relevant period, the Bank did not adapt its transaction monitoring system.

30. Throughout the relevant period, TDBNA utilized an automated transaction monitoring system to detect and generate alerts on suspicious transactions and activities. From at least 2014 to late 2022, TDBNA failed to implement any new transaction monitoring scenarios or make any substantive changes to the parameters of its existing transaction monitoring scenarios, despite significant unaddressed risks. For example, TDBNA did not have any scenarios to monitor changes and anomalies in a particular customer's transaction behavior, a standard indicator of suspicious activity, or any specific scenarios to monitor customers it deemed to be higher risk, such as money services businesses and precious metals dealers. And although TDBNA typically applied different dollar scenario thresholds to personal accounts and business accounts, the Bank did not apply different standards to different business accounts, meaning that a Fortune 500 company was subject to the same scenarios and dollar thresholds as a sole proprietorship, despite fundamental differences in the type and volume of activity.

31. These transaction monitoring deficiencies were exacerbated by TDBNA's failure to implement any new scenarios or materially modify any existing scenarios during the relevant period. As acknowledged in TDBNA's draft document titled, *New Transaction Monitoring Scenario Development Procedures (2017)*, which was never finalized, "[a] new transaction monitoring scenario may be required . . . if [an] existing transaction monitoring scenario does not cover the intended risk."

32. During the relevant period, US-AML employees escalated known gaps in the Bank's transaction monitoring system to GAML and US-AML management and proposed new or enhanced scenarios to address those risks. Individual-1 pointed to TDBNA's legacy technology

systems as a contributor to TDBNA's failure to implement or modify any scenarios. However, TDBNA not only failed to implement any automated solutions, it also did not create any effective manual transaction monitoring solutions or employ other stopgap measures until it could implement a more permanent solution.

33. Beginning as early as 2008, TDBNA severely limited the types of activity it screened through its transaction monitoring system. Specifically, after approximately 2011, TDBNA did not monitor *any* domestic ACH activity, most check activity, internal transfers between accounts at TDBNA, or numerous other transaction types. This decision had a profound effect on TDBNA's ability to monitor and report suspicious activity, as required by the BSA. As a result of this decision, between January 1, 2018, and April 12, 2024, TDBNA's automated AML monitoring failed to monitor 92% of transaction volume and 74% of transaction value, which corresponded to over 14.6 billion unmonitored transactions and over $18.3 trillion in unmonitored transaction value, which included a mix of lower- and higher-risk transactions.

34. Since 2008, TDBNA did not conduct any systematic analysis to review decisions not to monitor certain transaction types or whether they continued to be appropriate over the course of more than a decade. US-AML employees *did* repeatedly propose automated monitoring solutions to mid-level AML leadership to close this substantial gap. In 2012, after conducting a risk assessment, TDBNA elevated the AML risk of domestic ACH to "medium," largely due to the lack of monitoring, and this elevated rating remained in place during the entirety of the relevant period. In response, US-AML personnel proposed adding transaction monitoring scenarios to identify potentially suspicious domestic ACH activity. A GAML executive rejected this proposal. In 2019 and again in 2020, another US-AML employee highlighted the lack of domestic ACH and check monitoring to mid-level US-AML supervisors and unsuccessfully advocated for the

implementation of automated solutions. Throughout this period, certain individuals within GAML and US-AML including senior leadership, were aware of the lack of domestic ACH and check monitoring.

35. During the relevant period, while allowing the majority of its customers' activity to go unmonitored, TDBNA introduced new products and services and failed to address the AML risks associated with those products with any new or enhanced transaction monitoring scenarios.

a. In April 2017, for example, TDBNA began offering its individual customers access to Zelle, a mobile, person-to-person payment platform that allows its users to transfer funds between accounts at participating financial institutions. During the relevant period, TDBNA individual customers transferred over $75 billion in Zelle transactions, which was almost entirely unmonitored.

b. Although US-AML employees began assessing the money laundering risk associated with Zelle before its implementation, TDBNA failed to screen any Zelle activity through its transaction monitoring system until March 2020. In August 2020, TDBNA incorporated Zelle activity into two existing transaction monitoring scenarios covering suspicious wire activity in personal accounts but failed to recalibrate the scenarios to effectively identify suspicious Zelle activity, which typically involved lower transaction values and higher volumes than suspicious wire activity. In fact, those two scenarios only flagged personal customer activity exceeding $10,000 in deposits or $9,000 in transfers over a 5-day period, yet personal Zelle activity was capped at $10,000 during a rolling 30-day period. In other words, the scenarios captured activity that effectively could not occur through Zelle.

36. In July 2021, US-AML executives told the OCC during its annual examination that the Bank was conducting "scenario based monitoring" of Zelle activity based on the two scenarios

to which Zelle had been added. US-AML employees continued to identify Zelle as a gap in TDBNA's transaction monitoring program, with one employee noting that, "because we haven't been able to write a net new scenario," suspicious Zelle activity "gets lost in the much bigger $ wire category." Several US-AML employees continued to advocate to mid-level management for the implementation of appropriately calibrated scenarios to alert on suspicious Zelle activity, but GAML put the Zelle scenario project on hold in late 2021 because it was not "an exposed risk or regulatory need."

37. In 2015, the OCC instructed TDBNA to enhance its transaction monitoring program for high-risk customers, which were subject to the same scenarios and thresholds as the rest of TDBNA's customers despite their higher risk profile. In 2016, as part of that effort, the US-AML, GAML, and TD Bank Group technology teams began to develop new high-risk customer scenarios. That effort was put on hold in October 2016 by GAML executives due to a lack of resources. After being briefly revived in early 2017, this project was again put on hold, this time by Individual-1, partly due to "cost." Although US-AML leadership informed the OCC during its examinations in 2017, 2018, and 2019 that these scenarios were in development, TDBNA never implemented the required enhanced transaction monitoring of high-risk customers.

38. TDBNA left other significant gaps in its transaction monitoring program. For example, in or around 2011, TDBNA decommissioned several scenarios targeting large cash activity by businesses and other non-personal customers with the stated intention to test and recalibrate the scenario thresholds, identify potentially new parameters, and redeploy the scenarios. But the Bank did not do this. In fact, these scenarios remained offline from 2011 until late 2022, which allowed suspicious cash activity to be processed without alerts, including

hundreds of millions of dollars of transactions by two of the money laundering networks detailed below.

39. The limited changes TDBNA made to its scenarios during the relevant period almost exclusively—and intentionally—reduced the universe of alerts being generated and thereby lowered the associated cost of their review. Indeed, while TDBNA did not add any new transaction monitoring scenarios during the relevant period, it removed at least nine.

40. In February 2018, another U.S. bank entered into a negotiated resolution with the Department of Justice for its programmatic AML failures and failure to file SARs, the former of which was predicated, in part, on the bank's cessation of transaction monitoring scenario threshold testing. Senior US-AML executives were aware of this resolution and understood that banks must monitor their transactions for suspicious activity, with Individual-2 explaining to the AML Oversight Committee that "We always look at one of these actions and look at our own program and compare the conduct that has occurred. We look at our own processes to make sure nothing like this is happening. . . ." Specific to scenario threshold testing, Individual-2 asserted that "for each one of our scenarios we will do a lot of analysis and work below each threshold to see if SARs should have been filed. If we are seeing a certain percentage of SARs that would be filed, then we will look at whether we would lower that threshold on that particular scenario. … In contrast, [the U.S. bank] either ignored or discontinued that below the line threshold testing." Nevertheless, by the beginning of 2018, US-AML, along with its GAML technology partners, effectively stopped conducting threshold testing on its scenarios due to competing priorities and limited resources. As a result, from 2018 through 2022, TDBNA conducted threshold testing—what it referred to as "quantitative tuning"—on only one of its approximately 40 U.S. transaction monitoring scenarios.

41. In another example, throughout the relevant period, TDBNA maintained and regularly updated a list of "high-risk countries," which were jurisdictions found to have higher indicia of risk, including AML and terrorist financing risk. US-AML, however, only effectively monitored transactions involving what it dubbed "high high risk countries" ("HHRCs"), which were a subset of the high-risk country list and which were not updated after 2013, regardless of any changes to TDBNA's high-risk country list, updates to the Financial Action Task Force's[1] "grey list," or other geopolitical events. During this same period, GAML executives removed numerous countries from the HHRC transaction monitoring scenarios and only approved threshold changes that "would have no impact or lower the volume of false positives." In other words, GAML prioritized reducing alerts and the associated cost savings over identifying suspicious activity involving high-risk countries. Until at least December 2023, countries like the Dominican Republic and Jamaica were not included on the HHRC list, even though US-AML employees repeatedly identified suspicious ATM activity involving such countries.

GAML Operated under Budget Constraints

42. GAML's budget was a primary driver of its decisions about projects, hiring, staffing, and technology enhancements throughout the relevant period. GAML executives strove to maintain what TD Bank Group referred to as a "flat cost paradigm" or "zero expense growth paradigm," meaning that each department's budget, including GAML's, was expected to remain flat year-over-year, despite consistent growth in TD Bank Group's revenue over the relevant

[1] The Financial Action Task Force ("FATF") is an international policy-making and standard-setting body charged with safeguarding the global financial system from money laundering and terrorist financing. The "grey list" identifies countries that FATF determined to have strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing.

period. This budgetary pressure originated with senior bank executives and was achieved within GAML and US-AML by Individual-1 and Individual-2, both of whom touted their abilities to operate within the "flat cost paradigm without compromising risk appetite" in their self-assessments. GAML's base and project expenditures on US-AML were less in fiscal year 2021 than they were in fiscal year 2018 and were not sufficient to address AML deficiencies including substantial backlogs of alerts across multiple workstreams, despite TDBNA's profits increasing approximately 26% during the same period. In 2019, Individual-1 referred to the Bank's "historical underspend" on compliance in an email to the Group senior executive responsible for the enterprise AML budget, yet the US-AML budget essentially stayed flat. GAML and US-AML employees explained to the Offices that budgetary restrictions led to systemic deficiencies in the Bank's transaction monitoring program and exposed the Bank to potential legal and regulatory consequences.

43. At certain points throughout the relevant period, TDBNA postponed or cancelled proposed improvements to its transaction monitoring program, often to reduce AML costs. For instance, in August 2019, several US-AML and GAML executives, including Individual-2, met to discuss the fiscal year 2020 budget and identified several transaction monitoring projects to postpone, referring to them as "opportunities to reduce expenses for 2020/Opportunity to push out to future years." The group postponed a project designed to "Enhance Functionality and Scenario Development for U.S." because "new scenario development means new data and a lot of work effort." The group also postponed a project related to "Manual Monitoring," finding that it would require "new data feeds" and "scenarios" and there was "no capacity to do this." The Bank never completed either of these postponed projects.

Bank Employees Openly Discussed the Bank's Facilitation of Criminal Activity

44. TDBNA's failures to address emerging risks and new products and its focus on operational risk versus programmatic risk resulted in employees throughout the Bank discussing the efficacy of TDBNA's AML program. In October 2021, when asked by a colleague what "the bad guys" thought about the Bank's AML program, GAML's lead AML technologist and one of Individual-1's direct reports summarized the program as follows:

AML Technologist	what do the bad guys have to say about us
GAML Manager	Lol
GAML Manager	Easy target
AML Technologist	damnit
GAML Manager	Old scenarios ; old CRR ; tech agility is poor to react to changers
GAML Manager	Bottomline we have not had a single new scenario added since we first implemented SAS due to various issues with the install

45. Other employees, both in GAML and retail, consistently commented on the Bank's instant messaging platform about the Bank's motto, "America's Most Convenient Bank," and directly linked it to the Bank's approach to AML. For example, a US-AML employee noted that a reason the Bank had not stopped one of the below-referenced money laundering typologies was because "we r the most convenient bank lol." Similarly, when two US-AML employees discussed another one of the below-referenced money laundering typologies, as well as other customers engaged in potentially suspicious activity, the following conversation occurred:

Employee 1	:P why all the really awful ones bank here lol
Employee 2	because…
Employee 2	we are convenient

Employee 2	hahah
Employee 1	bahahahaha
Employee 1	that was their worst move evvvver

46. Others discussed cost and other impediments associated with developing new scenarios. For example, in both 2018 and 2020, an AML technologist sought to initiate scenario development projects, but both were ultimately deemed to be out of scope, decisions the AML technologist attributed directly to budgetary limitations. Also in 2020, a US-AML employee, in discussing an unfulfilled automated solution to an existing manual process, noted that GAML "can not properly code the scenario to give us what we want and its [sic] too much money to hire a coder …. Lol[.]"

TDBNA's AML Failures Allowed Millions In Illicit Funds To Flow Through the Bank

47. Multiple money laundering networks took advantage of TDBNA's deficient AML program and permissive procedures to launder at least $671 million in suspected illicit proceeds through TDBNA accounts.

48. Between January 2018 and February 2021, Da Ying Sze, who was known to TDBNA employees as "David," and his co-conspirators (collectively, "David's Network") moved approximately $474 million through TDBNA stores in New Jersey, New York, Pennsylvania, Maine, and Florida. According to David, who attempted to launder money through numerous financial institutions, TDBNA had by far the most permissive policies and procedures. As a result, TDBNA was where David chose to launder most of his funds. In February 2022, David pleaded guilty to engaging in more than $653 million in monetary transactions in property derived from a specified unlawful activity, operating an unlicensed money transmitting business, and bribing bank

employees. Four of David's co-conspirators similarly pleaded guilty to unlicensed money transmitting charges.

49. In furtherance of his scheme, David used nominees to set up shell companies and opened bank accounts in the names of those nominees and shell companies at TDBNA, or to use existing accounts that had previously operated without suspicious activity. David then laundered bulk cash through these TDBNA accounts, depositing up to millions of dollars of cash in a single day; immediately moved the funds out of the accounts using official bank checks and wire transfers; and conducted other transactions despite being neither an accountholder nor a signatory. David's Network also moved a substantial amount of illicit funds through TDBNA personal accounts, and in some instances David told TDBNA employees that he was using the personal accounts for business transactions because they incurred fewer bank fees. Throughout his money laundering scheme at TDBNA, David distributed over $57,000 in retail gift cards to TDBNA retail employees. According to David, the gift cards were meant to ensure that Bank employees would continue processing his transactions.

50. David's suspicious activity was obvious even to the casual observer. For example, the surveillance photograph below depicts David conducting a $372,000 cash transaction at a midtown New York store on July 21, 2020. David transacted in accounts that were not in his name. As depicted below, an account holder sat in the background not participating in the transaction while David, who was not the account holder, conducted the transaction. The account owner's lack of participation makes clear that while the account was opened in someone else's name, David actually controlled the account. That same day, David conducted a $290,000 cash transaction at a different TDBNA store. During these transactions, David purchased 14 official bank checks.

51. Throughout 2020, Individual-2 regularly received reports that aggregated and analyzed the Bank's CTR and monetary instrument activity. Within those reports, the extraordinary volume and value of David's Network's official bank check activity were repeatedly highlighted as substantial outliers. The February 2020 report called out two of the companies in David's Network for purchasing a total of $8.5 million in official bank checks, the highest amount of official bank checks at two different TDBNA stores. The report further noted that $8.3 million of those official bank checks were purchased with cash. Business and personal accounts linked to David's Network (but not held by David himself) were singled out in subsequent reports to Individual-2 throughout 2020 for outlier activity. Individual-2 stated that she did not review the reporting carefully because she incorrectly assumed that other US-AML executives were also receiving the reports, although she was the sole recipient. As a result, these reports did not initiate any additional investigation concerning David's Network.

52. TDBNA Retail employees at multiple levels understood and acknowledged the likely illegality of David's activity. In August 2020, one TDBNA store manager emailed another store manager and remarked, "You guys really need to shut this down LOL." In late 2020, another store manager implored his supervisors (several TDBNA regional managers) to act, noting that "[i]t is getting out of hand and my tellers are at the point that they don't feel comfortable handling these transactions." In February 2021, one TDBNA store employee saw that David's Network had purchased more than $1 million in official bank checks with cash in a single day and asked, "How is that not money laundering," to which a back-office employee responded, "oh it 100% is."

53. Retail employees also alerted US-AML personnel to David's suspicious activity through their submission of UTRs, which were the primary means for TDBNA retail employees to escalate potentially suspicious behavior to TDBNA's Financial Intelligence Unit, which assessed the UTR and fed it into the suspicious activity review stream, the primary means by which US-AML could be alerted to suspicious in-store conduct. Per TDBNA policy, employees that "identify an unusual activity or transaction or potentially suspicious conduct . . . must escalate or report it in accordance with [their] Business Unit procedures" through the submission of a UTR. Without retail employee submission of UTRs, it would be difficult for US-AML to know, for example, that a customer refused to provide identification during an in-store transaction or, as with David's Network, that a third party was regularly conducting transactions in multiple accounts that were not in their name.

54. For David's Network, the suspicious activity far outpaced the number of UTRs filed. Retail employees repeatedly failed to report David's suspicious transactions, including the deposit pictured above in paragraph 50. In the UTRs employees did file, the retail employees clearly communicated the gravity of the conduct. In a UTR from January 5, 2020, a retail employee

wrote that the activity "might be part of group that has been depositing extremely large amount of cash and possible laundering money." On September 9, 2020, a different retail employee succinctly reported to US-AML that, "EVERY DAY CUSTOMER DEPOSIT A LOT OF CASH." In another UTR from November 2020, a retail employee reported to GAML that they did "not feel comfortable doing their deposits knowing the activity is highly suspicious."[2]

55. The US-AML employees tasked with UTR intake and escalation were aware of David's Network, with one noting in July 2020 that "[t]hey have certainly been a thorn in our side for quite some time!!" The UTR team was regularly understaffed—in part due to the Bank's "flat-cost paradigm"—and the intake process was manual and laborious, which frequently resulted in backlogs. As a result, US-AML's UTR team tried to reduce the number of incoming UTRs, particularly on repeat subjects like David's Network that had already generated alerts. In August 2020, Individual-3 approved an updated procedure that allowed the UTR intake team to inform stores that additional UTRs were not required on specific customers unless the customers' unusual activity changed or continued beyond 60 days. This procedural change, which directly contravened TDBNA policies, resulted in multiple TDBNA stores being informed that no further UTRs were necessary on specific customers, including David's Network. Upon receipt of this guidance from US-AML, several retail employees assumed this instruction indicated that the activity was within the Bank's risk tolerance.

56. The limited universe of UTRs was exacerbated by the inaccurate CTRs the Bank submitted for activity involving David's Network, which almost uniformly failed to identify David as the conductor of the transactions. Consistent with the BSA, TDBNA policy required store

---

[2] Based on the UTRs from retail employees and the transaction monitoring alerts, the Bank eventually filed SARs on David's Network. These SARs failed to include David and only involved approximately 70% of the suspicious activity related to David's Network.

employees to collect information from the "person conducting transaction for another" and in training materials advised employees to identify the "conductor" in CTRs, i.e., "the person(s) who physically conducts the transaction." In practice, however, employees regularly identified only the TDBNA accountholder on the CTR form, which TDBNA enabled by prepopulating the accountholder information on the CTR form. For example, in the surveillance photo in paragraph 50, above, the corresponding CTR listed the TDBNA customers—including the shell companies, and their individual nominee owners who held the accounts on behalf of David—as the "person conducting transaction on own behalf," not David, the obvious conductor of the transaction.

57. This was not an isolated failure. TDBNA's CTR failures spanned numerous stores and dozens of employees. Of the hundreds of CTRs filed on activity in accounts linked to David's Network, indicia of David's involvement were included on only 20 CTRs. As a result, TDBNA willfully filed 564 materially inaccurate CTRs that did not identify David as the conductor of the transaction. These materially inaccurate CTRs, which spanned from June 2019 through February 2021 and covered transactions totaling $412,876,589, subverted the purpose of the CTR form and impeded law enforcement's ability to identify and prevent money laundering.

58. In addition, from March 2021 through March 2023, MLO-1 maintained accounts for at least five shell companies at TDBNA and used those accounts to move approximately $123 million in illicit funds through the Bank. Since their account-openings in 2021, TDBNA knew that these shell companies were connected because they shared the same account signatories. Retail employees submitted two UTRs highlighting the suspicious nature of MLO-1's activity, including that the cash deposits were "excessive for their type of industry." Despite these red flags, TDBNA did not file a SAR on MLO-1 until law enforcement alerted TDBNA to MLO-1's conduct in April

2022. By that time, MLO-1's accounts had been open for over 13 months and had been used to transfer nearly $120 million through TDBNA.

59. TDBNA's failure to file SARs on MLO-1 in a timely manner is attributable to the Bank's transaction monitoring failures. First, TDBNA's transaction monitoring system did not generate a single automated alert on MLO-1's primary deposit account (the "Management Account"), where the MLO deposited over $122 million in cash. By 2021, when MLO-1 first began to transact through TDBNA, TDBNA had long decommissioned its transaction monitoring scenario targeting large-cash deposits by business customers, as detailed above. Had this decommissioned scenario been active during the 13 months of MLO-1's activity, it would have generated approximately 161 transaction monitoring alerts on MLO-1's Management Account over the course of the $122 million in deposits.[3]

60. Second, TDBNA's transaction monitoring scenarios targeting "high-velocity" transactions (where the money moves out quickly after deposit) failed to monitor most transaction types, including the intrabank transfers utilized by MLO-1. Therefore, immediately after depositing a large sum of cash into the Management Account, MLO-1 was able to quickly transfer the funds to its other accounts at TDBNA without detection. This type of high-velocity transaction is a common indicator of money laundering. In mid-2019, a GAML employee identified this monitoring gap for high-velocity transfers, noting, "it does not appear there are scenarios focused on expedient money movement across all TD products." Although a remedial scenario was added to a scenario development list in early 2020, no such scenario was ever developed. Accordingly,

[3] The same transaction monitoring scenario, had it been operational, would have generated an additional 271 alerts on business accounts controlled by David's Network.

none of the high-velocity transfers from the Management Account to MLO-1's other TDBNA accounts, totaling approximately $120 million, generated an alert.

61. Third, while TDBNA identified the MLO-1 accounts as high-risk because they were allegedly involved in the precious metals business, TDBNA employed no enhanced transaction monitoring scenarios to identify suspicious conduct by such high-risk entities, although the accounts were subject to periodic reviews. This gap caused US-AML to receive fewer alerts than were warranted, given the highly suspicious nature of MLO-1's profile.

62. Additionally, beginning no later than 2018 and continuing through October 2023, TDBNA failed adequately to thwart a method of money laundering involving depositing funds into personal and business accounts in the United States and withdrawing cash at ATMs in Colombia (the "Colombian ATM Typology"). The Colombian ATM Typology, which FinCEN has designated as a risk for the financial industry,[4] persisted at TDBNA in part due to considerations that account restrictions could impair the customer experience and the Bank's failure to implement controls and procedures to enforce its AML policies. For example, TDBNA failed to implement appropriate internal controls to enforce its fifteen-debit card limit per business account and its requirement that customers be present during account opening and debit card issuance, which allowed insiders to provide dozens of ATM cards to money laundering networks. Further, TDBNA's fee structure for certain account types allowed money launderers to withdraw cash at Colombian ATMs without incurring any bank fees. As discussed below, the Colombian ATM Typology was also aided by the TDBNA Insiders.

---

[4] *See, e.g.*, FinCEN Advisory, *Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering*, FIN-2010-A001 (Feb. 19, 2010).

63. Between November 2019 and November 2022, a money laundering network ("MLO-2") used TDBNA to transfer over $39 million in illicit funds using the Colombian ATM Typology. In furtherance of this scheme, MLO-2 aggregated funds into bank accounts at various financial institutions, wired the funds to one of its approximately thirty TDBNA checking accounts, and then immediately withdrew the funds at ATMs in Colombia using debit cards. To facilitate these withdrawals, MLO-2 took advantage of TDBNA's deficient AML controls and paid kickbacks to an insider to obtain as many TDBNA debit cards as possible.

64. TDBNA accounts were particularly conducive to MLO-2's scheme for several reasons. First, some TDBNA stores did not enforce the requirement for debit card signatories to appear in person and instead allowed MLO-2 to present screenshots or photocopies of Venezuelan passports as identification. MLO-2 also reused the same Venezuelan passports across their TDBNA bank accounts, and sometimes used the same passport to obtain multiple debit cards for a single account. In some instances, representatives of MLO-2 were not required to provide any identification to obtain debit cards. Second, TDBNA would issue as many debit cards as MLO-2 requested for its business checking accounts, despite an internal policy establishing a 15-card limit per account. This allowed MLO-2 to obtain, in certain cases, up to 46 debit cards per TDBNA account and move money to Colombia in amounts 40 to 50 times higher than the daily withdrawal limit for personal accounts. Third, TDBNA's favorable fee structure for foreign ATM withdrawals as compared to its peer banks resulted in lower bank fees for MLO-2. As a result, approximately 70% of the total funds MLO-2 moved to Colombia were withdrawn using TDBNA accounts. An effective and properly resourced AML program would have identified and appropriately mitigated these risks.

65. MLO-2 was one of several money laundering organizations exploiting TDBNA accounts to move millions of dollars to Colombia. Some of this money laundering activity was facilitated by the TDBNA Insiders, who were responsible for opening accounts that transferred over $39 million to Colombia through a total of 194,940 ATM withdrawals.

66. TDBNA's failure to effectively manage its employee risk contributed to this insider misconduct—a result that was reasonably foreseeable to GAML and US-AML leadership in light of TDBNA's pervasive AML failures. The TDBNA Insiders opened personal and business accounts for individuals engaged in the Colombian ATM Typology, including MLO-2,[5] in exchange for bribes ranging from $50 to $2,500 per account. Insider-2 and others received these bribes directly into their personal accounts at TDBNA via Zelle—including some Zelle transfers directly from the TDBNA accounts the insider had opened. Insider-1 even used several of the illicit debit cards they issued to withdraw money directly from an ATM in their own TDBNA store.

67. In exchange for these bribes, the TDBNA Insiders opened accounts in the names of shell companies and nominee owners, often without the accountholder present; corresponded with the money launderers during the account's lifespan, often using their TDBNA email addresses; resolved any issues that arose while the accounts were active, including unblocking and replacing debit cards; and assisted with opening new accounts if and when an existing account was closed. For business accounts, the TDBNA Insiders were able to issue numerous debit cards—in some instances more than 50—for a single account, in contravention of TDBNA policy.

68. Despite numerous red flags, which the Bank did not appropriately act on, the Bank did not identify the TDBNA Insiders' misconduct, sometimes for years, until law enforcement intervention in late October 2023. For example, Insider-1, from a TDBNA store in New Jersey,

---

[5] Both Insider-1 and Insider-5 opened accounts for MLO-2.

opened numerous accounts for businesses with addresses listed in Florida. After Insider-1 was arrested by law enforcement, the Bank helped law enforcement identify similar misconduct by the additional insiders. Insider-2 opened dozens of accounts in the names of foreign citizens using a single address in Miami, Florida. Insider-3 issued dozens of debit cards to a number of business accounts and openly scheduled in-store pickups and other logistics with his TDBNA email address. Insider-4, after receiving text messages with personal information and corresponding Zelle payments, opened over one hundred accounts for individuals that were not present at account opening, including opening an account when the store was closed. Insider-5, who was linked to the Colombian ATM Typology during two different stints working at TDBNA, also opened accounts for individuals who were not present at account opening. Several of the TDBNA Insiders personally completed and signed tax documents and other account opening forms in furtherance of their misconduct.

69. In or around April 2019, TDBNA became aware of the Colombian ATM Typology, after the newly created Business Intelligence team within US-AML analyzed a series of accounts being used to funnel money to Colombia. This analysis explicitly likened the Colombian ATM activity to the FinCEN advisory noted above and identified patterns in the timing and location of the activity, including stores where the activity was most prevalent.[6] The analysis also revealed that certain accounts engaged in this activity were opened on the same day and using the same address. Business Intelligence provided a series of recommendations and next steps for addressing the Colombian ATM Typology, including that TDBNA: (i) engage in store-level training specific to the activity; (ii) investigate "inside jobs/involvements"; (iii) identify any similar accounts

[6] The list of stores Business Intelligence identified included the stores where Insider-3 and Insider-5 eventually worked.

beyond the 74 included in the initial analysis; and (iv) reconsider specific policies and procedures related to account openings and third-party cash deposits.

70. A version of this analysis was shared with the highest levels of GAML and US-AML, including Individual-2. On July 29, 2019, Individual-2 received this analysis and the proposed recommendations. In September 2019, a similar presentation was provided to the GAML Senior Executive Team, which was led by Individual-1 and included Individual-2. The same month, several mid-level US-AML executives convened to discuss the Colombian ATM Typology, during which they acknowledged that peer banks had instituted policies and safeguards that were closing the bad actors out of these banks and resulting in them seeking to use TDBNA, and agreed that the only way to prevent TDBNA from being used for this type of money laundering was for US-AML to influence retail policy change.

71. Yet, over the next eighteen months, TDBNA did not enact any of the changes or recommendations identified in Business Intelligence's analysis to address the Colombian ATM Typology. Although US-AML, including Individual-2 and their direct reports, discussed potential changes to retail policies and procedures with business-side personnel, such changes were ultimately abandoned due to the potential impact on the "customer experience" and the associated increased staffing requirements. Beginning in July 2020, in response to the Colombian ATM Typology, US-AML personnel sought to create an AML monitoring framework for business accounts with a high number of associated debit cards, but no such framework was implemented. During this period, US-AML identified and reported customers engaged in the Colombian ATM Typology. Nevertheless, the value of ATM withdrawals in Colombia using TDBNA accounts increased more than fivefold in three years, surging from $28.6 million in 2018 to $151.8 million

in 2021. In 2021 alone, a total of 12,227 TDBNA accounts had 675,570 ATM withdrawals in Colombia, a country in which TD Bank Group had no presence.

72. The Colombian ATM Typology continued at TDBNA until October 30, 2023, when—after law enforcement intervention—TDBNA began to identify and remove the five suspected insiders from its payroll and to institute systemic changes to prevent customers from engaging in the Colombian ATM Typology, including enhanced account opening controls, enhanced controls relating to debit card issuance, and reducing ATM withdrawal limits in certain countries, including Colombia.

73. Finally, even when TDBNA identified suspicious activity and decided to terminate customer relationships, the Bank often failed to carry out those terminations in a timely manner, thereby allowing billions of additional potentially suspicious funds to flow through the Bank. Throughout the relevant period, TDBNA maintained policies, procedures, and controls regarding the closure of accounts and termination of customer relationships based on AML risk, what TDBNA referred to as "demarketing." Due to historical understaffing—resulting in part from the Bank's "flat cost paradigm"—and repeated changes in demarketing procedures, TDBNA experienced frequent backlogs in its demarketing queue during the relevant period. In fact, for a significant portion of the relevant period, there was only one US-AML employee tasked with reviewing and dispositioning the thousands of annual Retail Requests to Close ("RTCs"), despite requests to Individual-2 to increase staffing on this project. These backlogs extended the period of time between the RTC submission and the actual account closure. From 2018 through 2021, on average, the demarketing process took nearly four months, with more complex cases averaging over five months from initial determination to account closure.

74. The practical effect of these persistent delays in demarketing was that, between 2018 and 2021, customers identified as outside of TDBNA's BSA/AML risk tolerance were regularly allowed to continue operating their accounts for months before they were finally closed. During the protracted timeframe between the initial determination and account closure, these customers conducted an additional $5.16 billion in transaction activity through their TDBNA accounts. In fact, accounts involved in David's Network and MLO-2 conducted a total of $168,375,555 in transaction activity *after* the Bank determined the accounts should be closed.